PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A1

(11) International Publication Number: WO 97/16904

(43) International Publication Date: 9 May 1997 (09.05.97)

(21) International Application Number: PCT/SE96/01396

(22) International Filing Date: 31 October 1996 (31.10.96)

(30) Priority Data:
9503841-0 31 October 1995 (31.10.95) SE

(71) Applicant *(for all designated States except US)*: NORD-BANKEN AB [SE/SE]; S-105 71 Stockholm (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: JOHANSSON, Anders [SE/SE]; Avstyckningsväg 40, S-175 43 Järfälla (SE).

(74) Agent: AWAPATENT AB; P.O. Box 45086, S-104 30 Stockholm (SE).

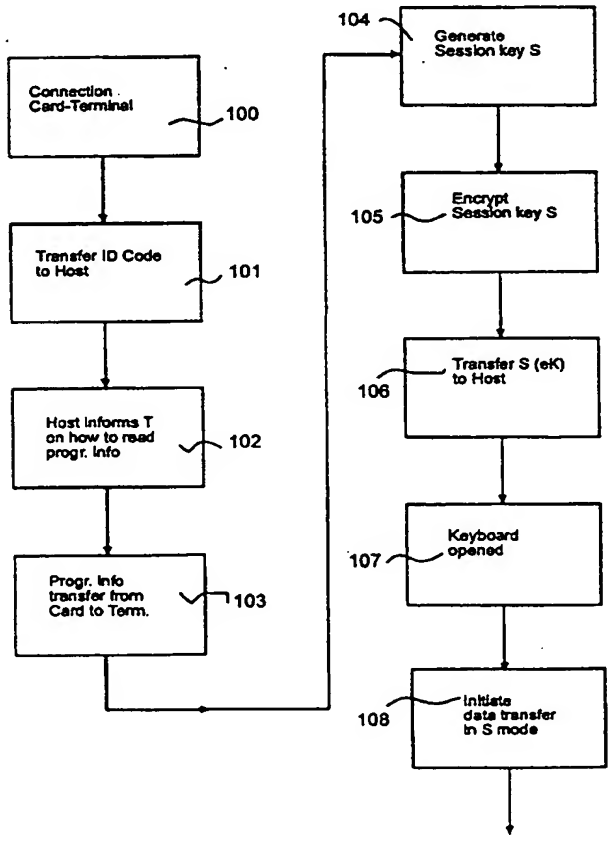
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
In English translation (filed in Swedish).

(54) Title: METHOD AND DEVICE FOR DATA COMMUNICATION

(57) Abstract

A method and a system for use for safe data transfer between a terminal which is controlled by an IC card (1), and a central unit (3), such as a central computer in a bank. The IC card (1) comprises card-specific program information which is used to control the interaction of the card with the terminal (2) in connection with adopting a safe system mode, and card-specific secret information which is used to cryptographically protect data transfers between the terminal (2) and the central unit (3) in a safe system mode. The card specific secret information is stored in such a manner that no read-out of it can be made from the card. The card-specific program information is transferred from the card to the terminal for the purpose of said control.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

METHOD AND DEVICE FOR DATA COMMUNICATION

Technical Field

The present invention relates to a method and a system for data communication between a central unit or host, such as a central computer in a bank, and a user unit comprising an IC card that the user carries and uses when he intends to carry out transactions involving communications with the host, and a terminal capable of communicating with the IC card and the host and acting as an interconnection link between them.

Background

It is presently known to use data transfer systems comprising IC card-controlled terminals and a host. It is likewise known to use, in these systems some kind of secret information to cryptographically protect transferred data.

Two principal disadvantages are found in the data transfer systems in use today. The first one relates to the fact that the terminals contain secret information which, on account of the physical availability of these terminals to the public, may be exposed to violation in the sense that an unauthorised person may try to read the secret information from the terminal. The second disadvantage is that since present standards on the configuration of IC cards, with the exception of such basic features as signal levels and the like, allow considerable degrees of freedom regarding for instance the memory addresses to which the data are to be allocated, the terminals normally are able to handle one type of card only.

Object of the Invention

The object of the present invention is to provide a method and a system solving or to a considerable extent eliminating the problems outlined above, thus providing increased flexibility with respect to the cards that may be used in the system and increased safety in the managing of the secret information.

Summary of the Invention

The purpose of the present invention is achieved by a method defined in claim 1 and a system defined in claim 11.

A basic concept of the invention is that at least sensitive data transfers between the user unit and the host are carried out in a separate safe system mode and that program-controlled realisation of the safe system mode is carried out by using card-specific program information contained in the card. The safe system mode means that data transfers are carried out in such a manner that unauthorised persons cannot distort or manipulate transfered data without such interference being discovered. For this purpose, secret information in the user unit and in the host is made use of. The teh inintiation of communication between the card and the terminal is carried out in so-called normal system mode.

Cards used in accordance with the invention contain card-specific program information transferred to and used by the terminal in connection with the establishment of a safe mode.

In accordance with the present invention the "resident" information contents in the terminal is no more extensive than is absolutely necessary. Each card carries program information which is specific to the individual card and which is transferred to the terminal. Since the card-specific program information is transferred to the terminal the latter need not contain "resident" program

information that is specific to each individual card or card type.

This makes it possible to use in the system, cards that are configured in different ways without it being necessary for the terminal to contain considerable software, and for example several card issuers may use the same set of terminals without it being necessary that the terminal contains, or that the other card issuers have knowledge of, the software that a specific card issuer uses in order that a safe system mode be adopted.

The system in accordance with the invention allows the terminal to be made both inexpensive and "flexible" in the sense that without difficulties it is possible to adapt the unity card/terminal to include cards that are configured differently without the terminal having to be changed or be provided with new "resident" program information.

Transfer of card-specific program information from the card to the terminal is effected, in accordance whit a preferred embodiment, under the controll of the host the actions of which are based on card-identifying information or a code transferred from the user unit. However, it is obviously possible that this may be effected by the terminal and the card without involving the host.

Cards used in accordance with the invention likewise contain card-specific secret information which is used to produce cryptographical protection of data transfers and which is stored in such a way that it cannot be read out from the card.

In accordance with a preferred embodiment the card-specific secret information is used to encrypt (in the widest sense), by means of an algorithm, preferably the so-called DES algorithm, a generated session key, preferably in the form of a random number which is then transferred to the host in encrypted form. This session key is then used to cryptographically protect data

transferred between the user unit and the host in a safe system mode.

The above-mentioned session key is erased in the user unit at the latest the next time contact is established between an IC card and the terminal, although it is possible to effect such erasure, for instance in response to a specific command while contact is still being maintained, because it is desired to begin a new session, or when the contact between the card in question and the terminal is interrupted.

Obviously it is likewise possible to use card-specific secret information as such in order to cryptographically protect data transferred between the host and the user unit in a safe system mode, i.e. that the secret information is used as a cryptographic key, either in an encryption algorithm or in an authentication algorithm.

In accordance with a preferred embodiment, the terminal comprises a keyboard which may be used only in a safe system mode.

In order to protect data transferred on an open line or in another medium accessible to unauthorised persons various different cryptographical techniques are used. A common method is to first encrypt data which are then transferred and finally decrypted. The reverse order is also possible, i.e. to first decrypt data, then transfer them and finally encrypt the transferred data which are then retrieved in cleartext. Both these techniques obviously may be used in connection with the invention. In the case of for instance a random number which is adopted to create an encryption key for an encryption algorithm it is possible to instead transfer the random number in cleartext and to then encrypt/decrypt it and later use the result as an encryption key. Also this technique may be used in connection with the invention, which thus is not limited to use in connection with the

cryptographic technique described herein in detail. Symmetrical as well as asymmetrical encryption systems may be used.

Brief Description of the Drawings

Fig. 1 is a schematic block diagram relating to one embodiment of a system in accordance with the present invention.

Fig. 2 illustrates a flow chart of measures to be taken in accordance with a preferred embodiment before initiation of data transfers between the user unit and a host in a safe system mode.

Fig. 3 illustrates the manner in which an encryption key is generated and encrypted in accordance with one embodiment of the present invention before the encryption key is transferred to the host.

Fig. 4 illustrates the authentication of messages (data) in accordance with a preferred embodiment of the present invention.

Fig. 5 contains a list of the different varieties of generation of code keys and transfer thereof to the host.

Figs 6a-6h are flow charts illustrating the varieties listed in Fig. 5.

Detailed Description of Embodiments of the Present Invention

In the following a system will be described with reference to Fig. 1 which system is designed for safe data transfers and which comprises a user unit, comprising an IC card 1, a terminal 2, and a central unit (host) 3.

The IC card 1 comprises card communication means 4 that are placed in contact with terminal communication means 5 to establish a connection for data transfers between the IC card 1 and the terminal 2.

In addition, the IC card 1 comprises first card memory means 9 for storing card-specific program information to be transferred to the terminal 2; second card memory means 10 for storage of card-specific secret information in such a way that it cannot be read out from the card; a memory means 16 for storage of a card-identifying code; and a processor 15 containing required program information to allow execution of the required cryptographic processing, in this case encryption, and generation of a session key before the latter is transferred to the host 3, as will be described further on.

The terminal 2 comprises a terminal communication unit 6 in communication with the central communication unit 7 associated with the host 3, in order to allow data transfers between the host 3 and the user unit, and a key generating means 13, in the form of a random number or pseudo random number generator for generation of a session key to be transferred to the host in an encrypted state and to be used for authentication of messages to be transferred between the user unit and the host 3, as will also be described later on. The terminal 2 comprises storage means 14 to store the session key.

In accordance with another preferred embodiment no key generating means is used in the terminal but the generation of the key instead takes place in the processor 15 in the card.

The terminal 2 and the host 3 in addition comprise control means 8, 18 to control the transfer of the system to the safe system mode which in accordance with the preferred embodiment is considered to have been adopted once the session key has been transferred to the host. In this mode data transfers between the terminal 2 and the host 3 take place in such a manner that data that are being transfered are protected (cryptographic authentication) by means of the session key that has been transferred to the host. In addition, the terminal 2

comprises read-out means 11 for read-out of the card-specific program information in said first card memory means 9, the read-out program information being stored in and used by program executing means 12 in the terminal 2 in order to control interaction between the terminal 2 and the IC card 1.

Fig. 2 illustrates in the form of a flow chart the manner in which the IC card, the terminal and the host cooperate in accordance with one embodiment before data transfer in a safe system mode is initiated, a process to be described in closer detail in the following with reference to Fig. 4.

In step 100, the IC card 1 is inserted in the terminal 2, whereby contact is established between said terminal communication means 5 and said card communication means 4. In step 101, an ID code stored in said memory means 16 is transferred via terminal 2 from the user unit IC card to the host 3. In step 102, on the basis of verification of the card type, i.e. the card configuration, the host 3 informs the terminal 2 on how its read-out means 11 are to proceed to read out the card-specific program information from said first card memory means 9. In accordance with a preferred embodiment, data transferred from the host contains information on the address where the read-out is to begin. In step 103, the card-specific program information is read from card 1 to terminal 2. In step 104, a random number is generated in said key generating means 13, said random number to be used as a session key in a sealing process while using a Message Authentication Algorithm (MAA). In step 105, the session key in the IC card is encrypter in said encryption means 15 using the secret information contained in the second card memory 10 of the IC card 1. In step 106, the session key is transferred in encrypted state to the host 3. Steps 104, 105 and 106 are illustrated in closer detail in Fig. 3. In step 107, a keyboard associated with the terminal 2 is opened for

use. In step 108, data transfer is begun in the now adopted safe system mode.

In the following, the description will be made with reference to Fig. 3. In accordance with the preferred embodiment a random number is generated in the terminal to be used as a key in an MAA process to authenticate messages (i.e. data) transferred from the user unit to the host and vice versa. This random number is then encrypted in the card in a DES encryption algorithm, using the secret information (DES key) in said second card memory means 10 (Fig. 1) as the encryption key in order to be transferred in encrypted state (the encrypted random number is designated by eK) via the terminal to the host 3, wherein it is decrypted and used as a session key in an MAA.

In Fig. 4 is exemplified the manner in which data transfers and authentication of data are carried out in a safe system mode in accordance with the preferred embodiment. The encrypted random number eK, having been transferred from the user unit, is decrypted in the host by means of a key stored in the host, said key depending on the card that is being used and being identical with the one in said card. The decrypted random number is then used as an MAA key together with a message to be transferred to the user unit and a message serial number, in an MAA in order to generate a cryptographic check sum, Message Authentication Code (MAC), which is added to and used to authenticate the message. The MAC will have a different appearance in successive messages during one and the same session (also when their contents are the same, since they have received different serial numbers). Thus, a flow of data is transferred, containing the message, the serial number, in cleartext, and a MAC.

In the user unit an MAA check is carried out to verify the message received while using the MAA key in the terminal, i.e. the random number, or in other words, a check to verify whether the message has been

manipulated on its way from the host to the user unit. The check comprises a corresponding computation of a MAC and a comparison thereof with the MAC received together with the message, to determine coincidence.

When the user unit is to transfer a response message to the host one proceeds in a corresponding manner, i.e. on the basis of the random number, the response, and the serial number transferred from the host a new MAC is computed, which is added to the flow of data formed by the response from the user unit to the host and the latest serial number transferred from the host. The host then performs an MAA check of the transfered response in order to check that the response has not been manipulated on its way between the user unit and the host. Further message transfers may then be carried out in the same way.

Fig. 5 is an account of a number of possible modifications 1-8 of random number generation and protection of random numbers that may be used in connection with the present invention. Four cases (1,3,5,6) are shown in which the random number used as a session key is generated in the terminal and four cases (2,4,7,8) wherein the random number is generated in the card. In addition, four different varieties are shown of the forms in which the corresponding session key is used for cryptographic protection respectively is transferred to the host.

Figs 6a-6h show the eight various cases accounted for in Fig. 5 in more detail. The various steps illustrated for each case are indicated by numeral references placed inside white rectangular boxes. Each Figure illustrates the situation occurring when a user has inserted his card in the terminal and the system is about to accomplish a safe mode. It appears from the Figures that steps S1-S5 are identical for all eight varieties. In step S1, the central unit (Host) commands the terminal (Terminal) to read out the identification number of the card to verify whether the card is associated with the

host in question and, when the verification is positive, to supply the encryption key which is associated with the card and which is to be used in the host to encrypt or decrypt the random number (session key), depending on in which form the key has been transferred to the host. In step S2, the terminal transfers the read-out card number to the host. In all eight cases, the host makes sure that the card has been issued by the user of the host, whereupon in step S3 it orders the terminal to begin to assume a safe mode. In steps S4 and S5 the terminal executed the program sequence that is its resident program information, i.e. to read and fetch the card-specific program information from a file (SMIB) in the card. The rest of the steps to be executed in order for a safe mode to be assumed is governed by the contents of SMIB, i.e. the card-specific program information. This shows that a comparatively simple and thus inexpensive terminal (in principle capable only of reading out a file from an IC card), when used in a system in accordance with the present invention, may achieve an astonishing degree of flexibility with respect to its ability to interact with cards that are configured in different ways. The first case illustrated is the one shown in Fig. 3, i.e. the random number to be used as a session key is generated in the terminal and is encrypted in the card, in step S6 before being transferred to and stored in the terminal in step S7, the terminal finally, in step S8, sending the encrypted random number to the host, whereupon data transfer in safe system mode may be started in accordance with Fig. 4.

In accordance with the second case illustrated the following steps are performed, in addition to steps S1-S5 already described, viz.: in step S62 the terminal orders (in accordance with the contents of the corresponding SMIB) the card to generate a random number; the card generates and sends a random number to the terminal wherein it is stored, in step S72; in step S82 the termi-

nal orders the card to encrypt the generated random number; the card encrypts the random number and transmits it in encrypted state to the terminal; in step S102, finally, the terminal transmits the encrypted random number to the host, whereupon data transfer in safe system mode may start in accordance with Fig. 4.

In the third case illustrated, the following steps are executed in addition to steps S1-S5 already described, viz.: in step S63 the terminal generates and stores a random number and orders the card to decrypt the random number: in step S73 the decrypted random number is transferred to the terminal; and in step S83 the decrypted random number is transferred to the host. When the random number (session key) reaches the host it should not be decrypted before use but be encrypted in order to provide the key in cleartext, and otherwise data transfers are commenced in a safe system mode in same manner as illustrated in Fig. 4.

In the fourth case illustrated the following steps are executed, in addition to steps S1-S5 already described, viz.: in step S64 the card is ordered to generate a random number; in step 74 this random number is transferred to and stored in the terminal; in step S84 the terminal orders the card to decrypt the random number; in step S94 the card sends the decrypted random number to the terminal; and in step S104 the decrypted random number is sent to Host. When the random number (session key) reaches the host it shoould not be decrypted before use but be encrypted to provide the key in cleartext and otherwise the data transfer in a safe system mode commences in the same manner as illustrated in Fig. 4.

In the fifth case illustrated the following steps are executed, in addition to steps S1-S5 already described, viz.: the terminal generates a random number which is transmitted in step S85 to the host in cleartext and which in step S65 is encrypted by the card; in step S75 the encrypted random number is transferred to and

stored in the terminal. Because there is an encrypted session key in the terminal and because the session key has been transferred to Host in cleartext it is necessary, in order to establish data transfer in safe system mode, to encrypt the session key in Host before it can be used.

The sixth case illustrated is distinguished from the fifth case only in the respect that whenever encrypting is effected in the fifth case decrypting now is to be performed.

In the seventh case illustrated the following steps are executed, in addition to steps S1-S5 already described, viz.: in step S67 the terminal orders the card to generate a random number which in step S77 is transferred to the terminal; in step S107 this random number is transferred in cleartext to the terminal and in step S87 the card encrypts the random number; in step S97, finally, the encrypted random number is transferred to and stored in the terminal. Because there is an encrypted session key in the terminal and because the session key has been transferred to Host in clear text it is necessary, in order to establish data transfer in safe system mode, to encrypt the session key in Host before it may be used.

The eighth case illustrated is distinguished from the seventh one only in the respect that whenever encrypting is effected in the seventh case decrypting now is to be performed.

One example of a set of the card-specific program information being transferred from the card to the terminal and producing the generation of a session key and transfer thereof to the host in accordance with variety 1 in Fig. 5 (Fig. 6a) may contain the following sequence of commands; OPEN (open up the file in the card containing the card-specific secret information, allowing it to be used as an encryption key in an encryption algorithm), RANDOM (generate a random number in the key-generating

means 13 of the terminal in accordance with the instructions contained in the command and storage of said number in the terminal storing means 14), CRYPT (read over the random number to the card and encrypt the random number in the card using a conventional encryption algorithm defined in and executed by the processor 15, and the encryption key), READ (read out the encrypted random number to the terminal) and TRANS (transfer the encrypted random number to host).

It should be understood that the commands and functions defined are only of an exemplifying nature and that they may be implemented in a large number of different ways and in a large number of different program languages. The methods of implementation of the functions used in the embodiments in accordance with the present invention in program code must be considered self-evident to those skilled in the art when reading the present invention and therefore they will not be described in more detail herein.

CLAIMS

1. A method of transferring data between a user unit comprising a terminal and an IC card which is placed in communication with the terminal, and a central unit, such as a central computer located at a producer of services, preferably a bank, secret information being used in the user unit and the central unit to protect data transferred between said units, c h a r a c t e r i s e d in that the user unit is made to operate in a safe system mode involving safe data transfer between the user unit and the central unit in the sense that unauthorised persons cannot gain knowledge of the transferred data and/or that it is possible to verify whether transferred data have been distorted or been replaced during the transfer, in that card-specific program information in the card is used to control the terminal as the latter interacts with the card in connection with the user unit being made to operate in a safe system mode, the card-specific program information being transferred to the terminal to be utilised in connection with said control, and in that safe data transfers are effected while making use of card-specific secret information in the IC card, the use of the card-specific secret information for cryptographic protection being effected in such a manner that the card-specific secret information never leaves the card.

2. A method as claimed in claim 1, wherein operations initially being carried out in a normal system mode in which communication is established between the terminal and the card and in which the card-specific program information is transferred to the terminal.

3. A method as claimed in any one of claims 1-2, wherein a card-identifying code being transferred from the user unit to the central unit, on the basis of which code said central unit instructs the user unit on the

manner to be adopted for the transfer of the card-specific program information from the card to the terminal.

4. A method as claimed in any one of claims 1-2, wherein the transfer of the card-specific program information is carried out on the basis of information contained in the terminal and/or the IC card before communication is established therebetween.

5. A method as claimed in any one of claims 1-4, wherein a session key is created in the user unit for use in the transfer of data in a safe system mode, said session key being encrypted or decrypted in the IC card, and wherein said session key is transferred to the central unit in an encrypted or decrypted form.

6. A method as claimed in any one of claims 1-4, wherein a session key is created in the user unit, said session key being transferred to the central processing unit in cleartext, whereupon said session key is encrypted or decrypted in the central processing unit and the IC card, to be used in an encrypted or decrypted form in the transfer of data in a safe system mode.

7. A method as claimed in claim 5 or 6, wherein the session key is a random number which preferably is generated in the terminal.

8. A method as claimed in any one of claims 5-7, wherein the session key in the user unit is erased as soon as connection between the card and the terminal is interrupted.

9. A method as claimed in any one of claims 5-7, wherein the session key in the user unit is erased as soon as a new connection is established between the terminal and an IC card.

10. A method as claimed in any one of the preceding claims, wherein input of information via a keyboard associated with the terminal may be effected only in a safe system-operational mode.

11. A system for transfer of data, comprising a user unit (1, 2) having an IC card (1) and a terminal (2), and a central unit (3), said card (1) comprising card communication means (4) for communication with the terminal (2), the terminal (2) comprising terminal communication means (5) for communication with the card (1), and a terminal communication unit (6) for communication with the central unit (3), said central unit (3) comprising a central communication unit (7) for communication with the terminal (2), and the user unit (1, 2) and the central processing unit (3) comprising secret information that is used to cryptographically protect data transfers between said units, c h a r a c t e r i s e d in that the IC card (1) comprises first card memory means (9) for storage of card-specific program information, and second card memory means (10) for storage of card-specific secret information which is used to cryptographically protect data transferred between the user unit and the central unit (3) in a safe system mode, said second card memory means (10) being configured in such a manner that said secret information cannot be read out from the card (1), that the terminal (2) comprises terminal read-out means (11) for reading the contents of said first card memory means (9) and program executing means (12) arranged, while utilising the read-out card-specific program information, to control the interaction between the terminal (2) and the IC card (1) in order to establish the safe system mode.

12. A system as claimed in claim 11, wherein the user unit comprising key generating means (13) arranged to generate a session key, and storage means (14) for storing such a session key, and wherein the IC card (1) comprises processing means (15) arranged to cryptographically protect the session key which said terminal communication unit (6) is arranged to transfer to the central unit.

13. A system as claimed in claim 12, wherein said key generating means (13) being a random number generator or a pseudo random number generator.

14. A system as claimed in claim 12 or 13, wherein said key generating means (13) are arranged in the terminal (2).

15. A system as claimed in claim 12 or 13, wherein said key generating means forms an integrated part of said processing means (15).

16. A system as claimed in any one of claims 12-15, wherein the user unit is arranged to erase the session key in the user unit as soon as connection between said card communication means (4) and said terminal communication means (5) is interrupted.

17. A system as claimed in any one of claims 12-15, wherein said user unit is arranged to erase the session key in the user unit as soon as new connection is established between said card communication means (4) and said terminal communication means (5).

18. A system as claimed in any one of claims 11-17, wherein the IC card (1) comprises memory means (16) for storage of card-identifying information or a card-identifying code arranged to be transferred to the central unit (3), said central unit being arranged, while being guided by said code or information, to instruct the user unit (1, 2) of the manner in which the contents of said first card memory means (9) are to be read out.

19. A system as claimed in any one of claims 11-18, wherein the user unit comprises a keyboard for input of data into the system, said keyboard being arranged to be operative only when the system is in a safe system mode.

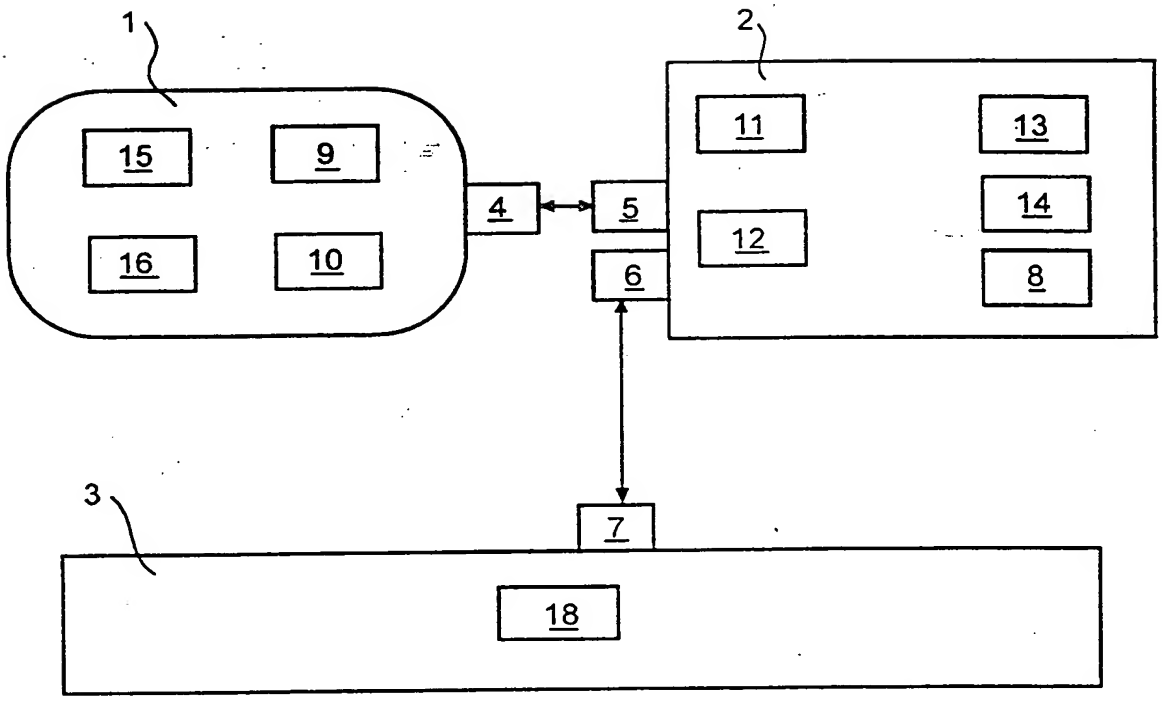


Fig. 1

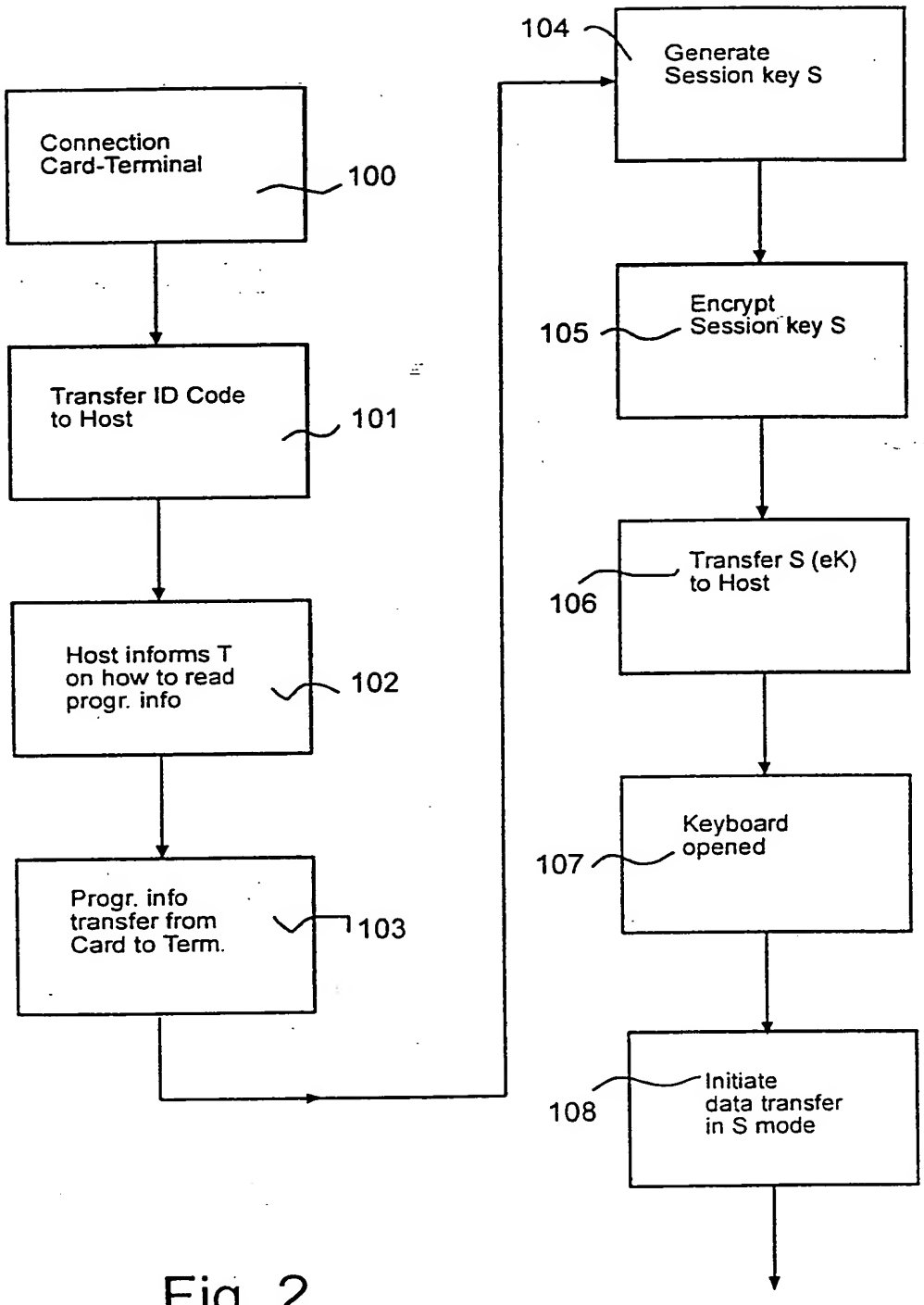

Connection Card-Terminal
100
Transfer ID Code to Host
101
Host informs T on how to read progr. info
102
Progr. info transfer from Card to Term.
103
104
Generate Session key S
105
Encrypt Session key S
106
Transfer S (eK) to Host
107
Keyboard opened
108
Initiate data transfer in S mode

Fig. 2

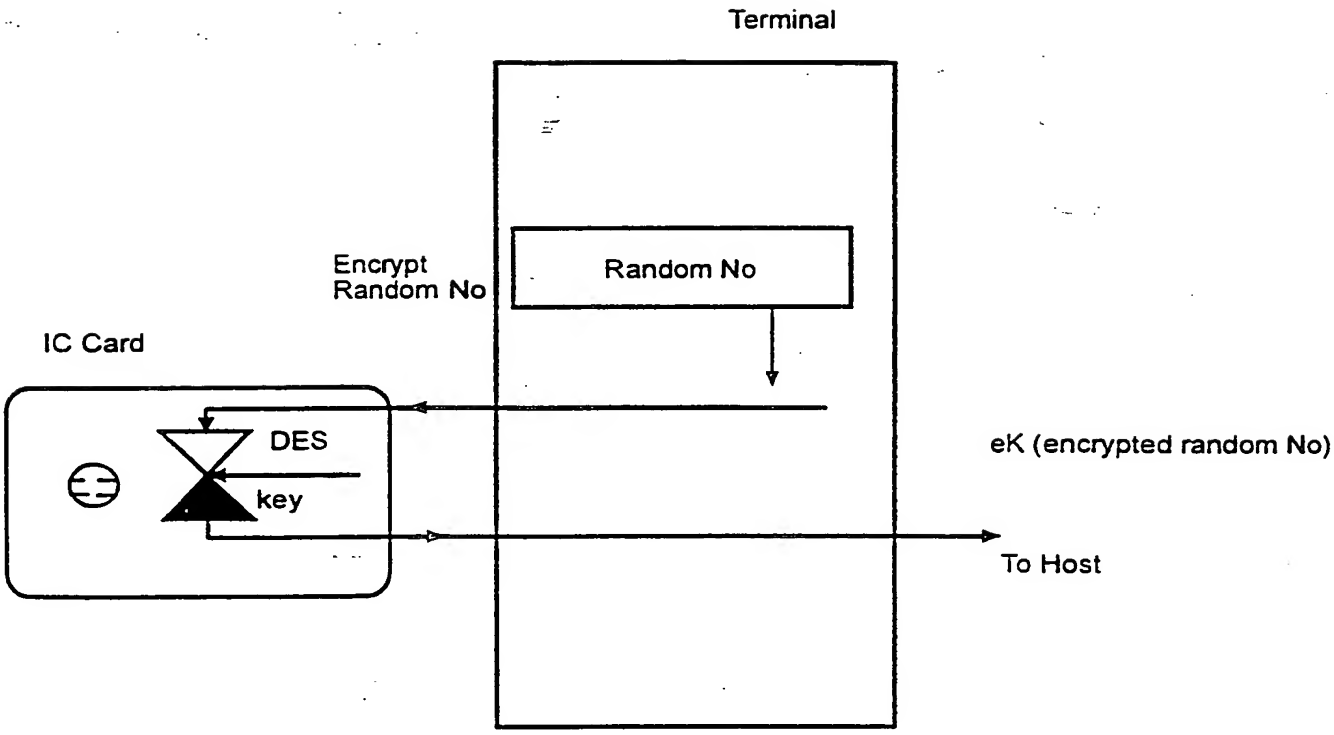

Terminal
Encrypt
Random No
Random No
IC Card
DES
key
eK (encrypted random No)
To Host

Fig. 3

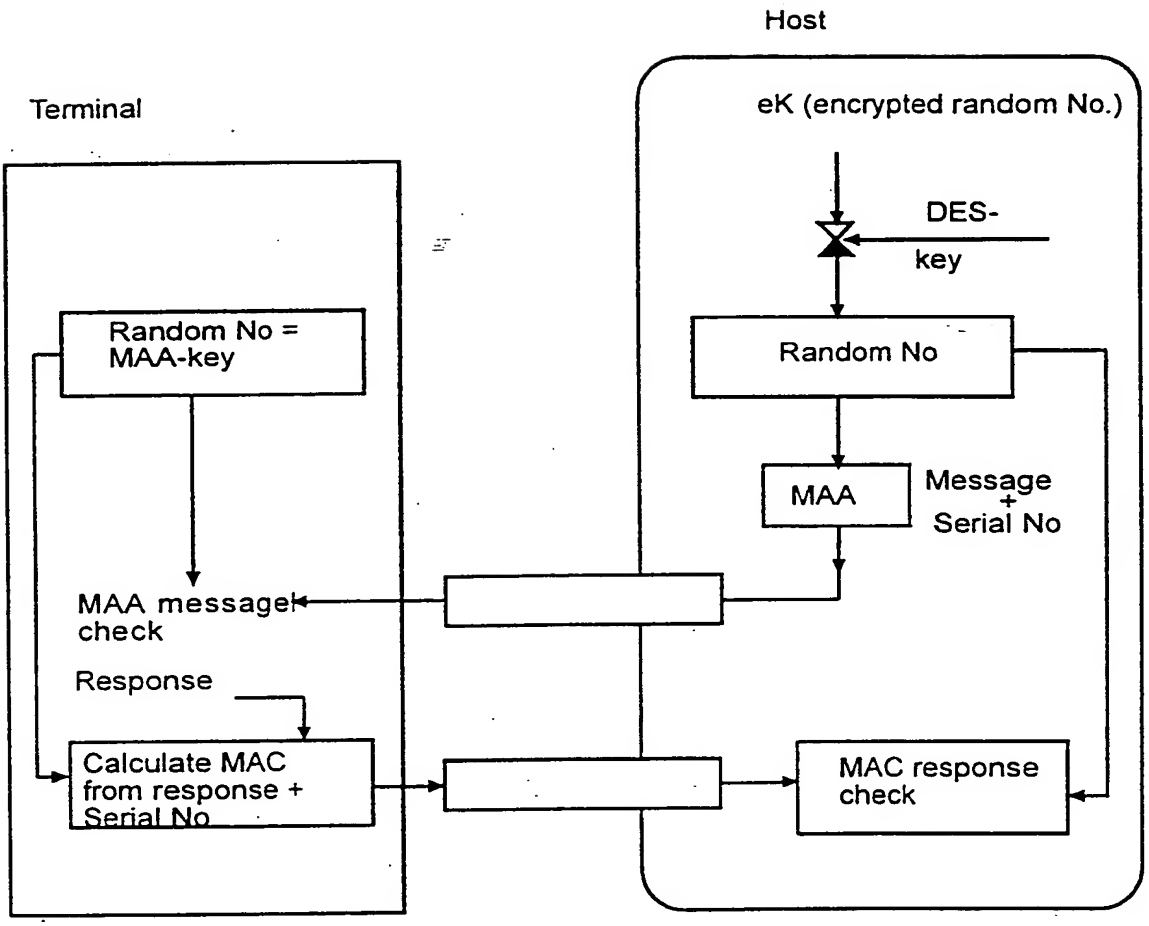

Host
Terminal
eK (encrypted random No.)
DES-
key
Random No =
MAA-key
Random No
MAA
Message
+
Serial No
MAA message
check
Response
Calculate MAC
from response +
Serial No
MAC response
check

Fig. 4

Variety	Generate Ranom No in	Store in Terminal and use Random No	Send Random No to Host	Prior to use in Host. received value to be
1	Terminal	In Cleartext	Encrypted	Decrypted
2	Card	In Cleartext	Encrypted	Decrypted
3	Terminal	In Cleartext	Decrypted	Encrypted
4	Card	In Cleartext	Decrypted	Encrypted
5	Terminal	Encrypted	In Cleartext	Encrypted
6	Terminal	Decrypted	In Cleartext	Decrypted
7	Card	Encrypted	In Cleartext	Encrypted
8	Card	Decrypted	In Cleartext	Decrypted

Fig. 5

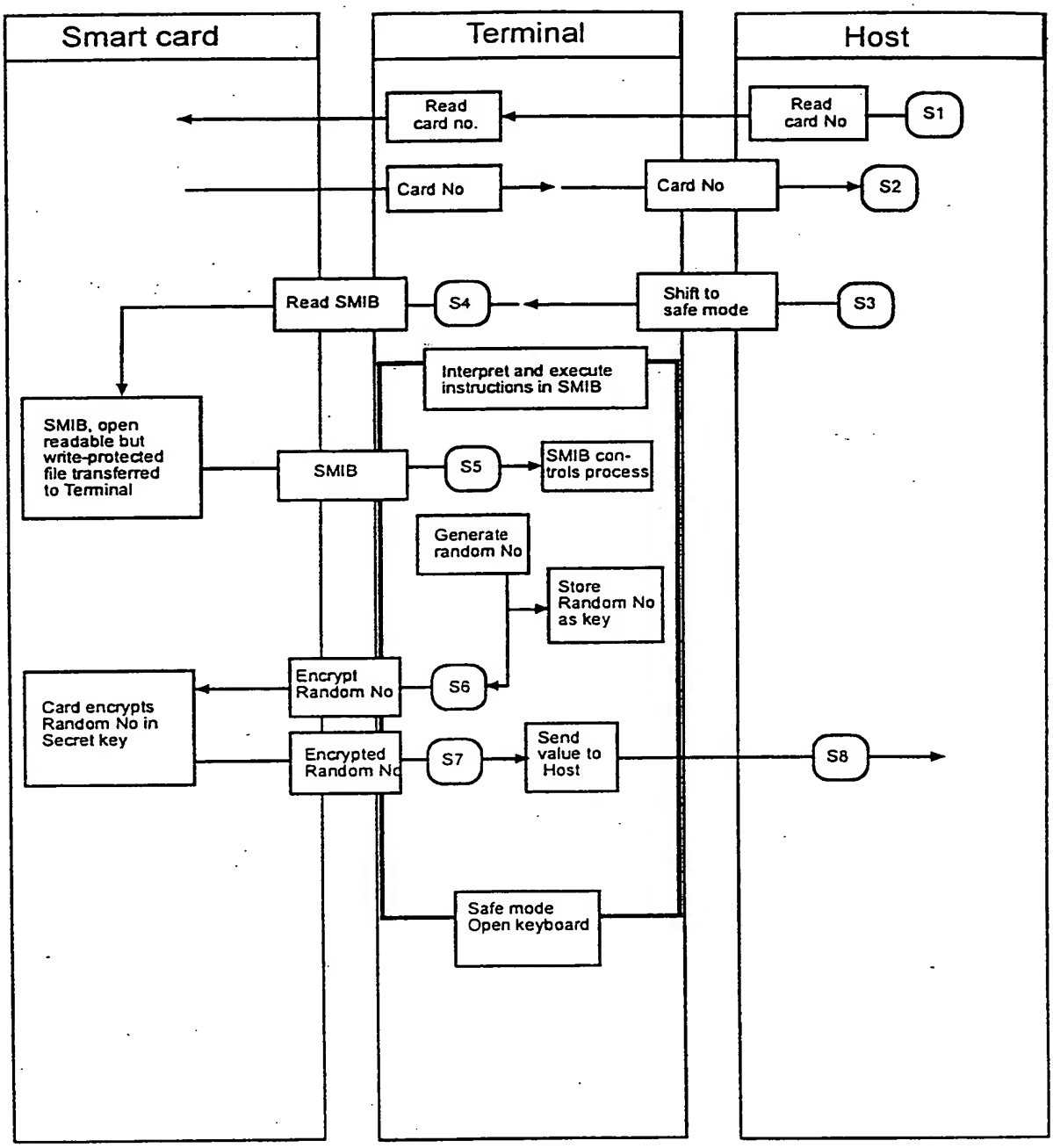

Smart card
Terminal
Host
Read card no.
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to Terminal
SMIB
S5
SMIB con-trols process
Generate random No
Store Random No as key
Encrypt Random No
S6
Card encrypts Random No in Secret key
Encrypted Random No
S7
Send value to Host
S8
Safe mode Open keyboard

Fig. 6a

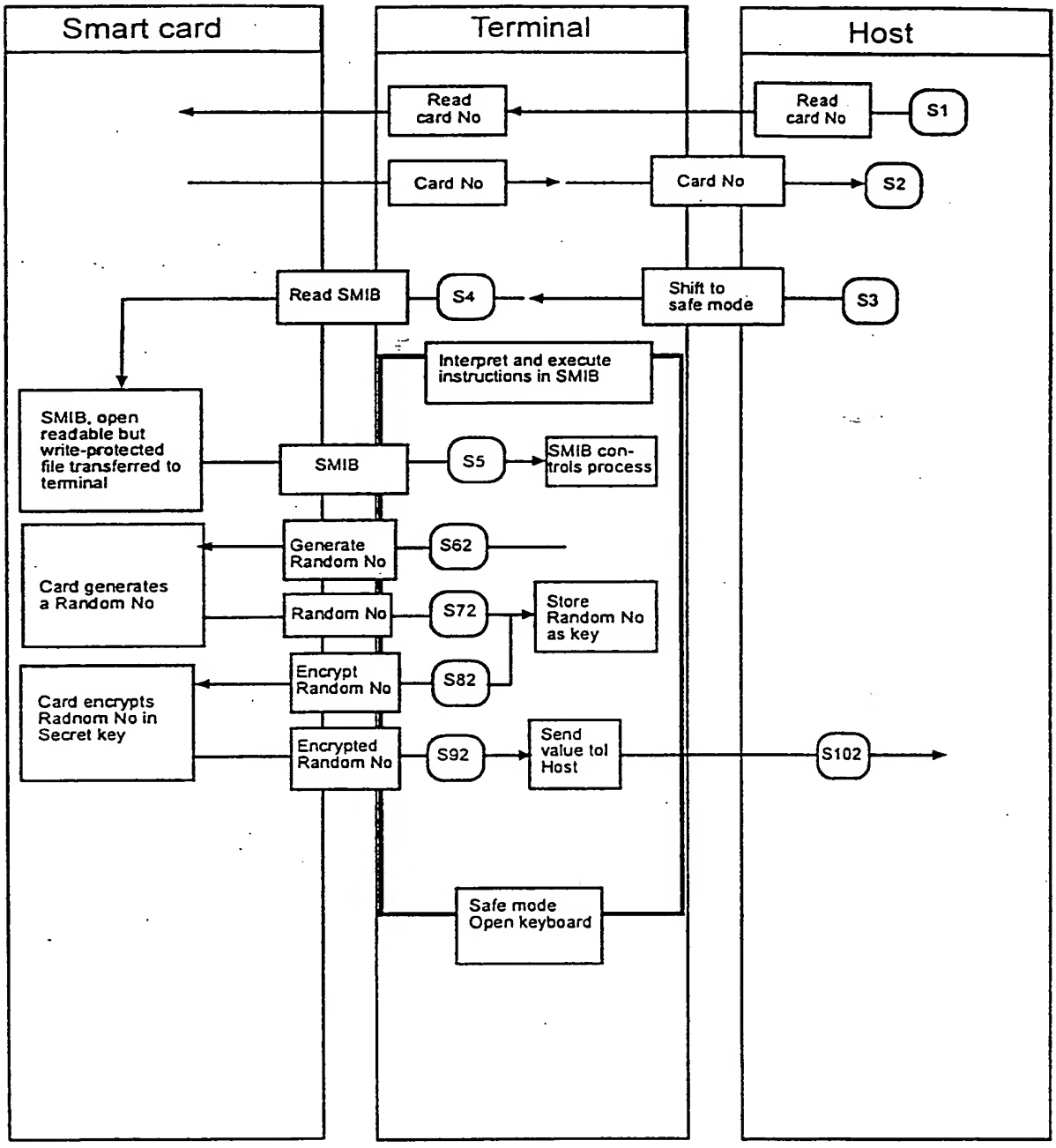

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB con-trols process
Generate Random No
S62
Card generates a Random No
Random No
S72
Store Random No as key
Encrypt Random No
S82
Card encrypts Radnom No in Secret key
Encrypted Random No
S92
Send value tol Host
S102
Safe mode Open keyboard

Fig. 6b

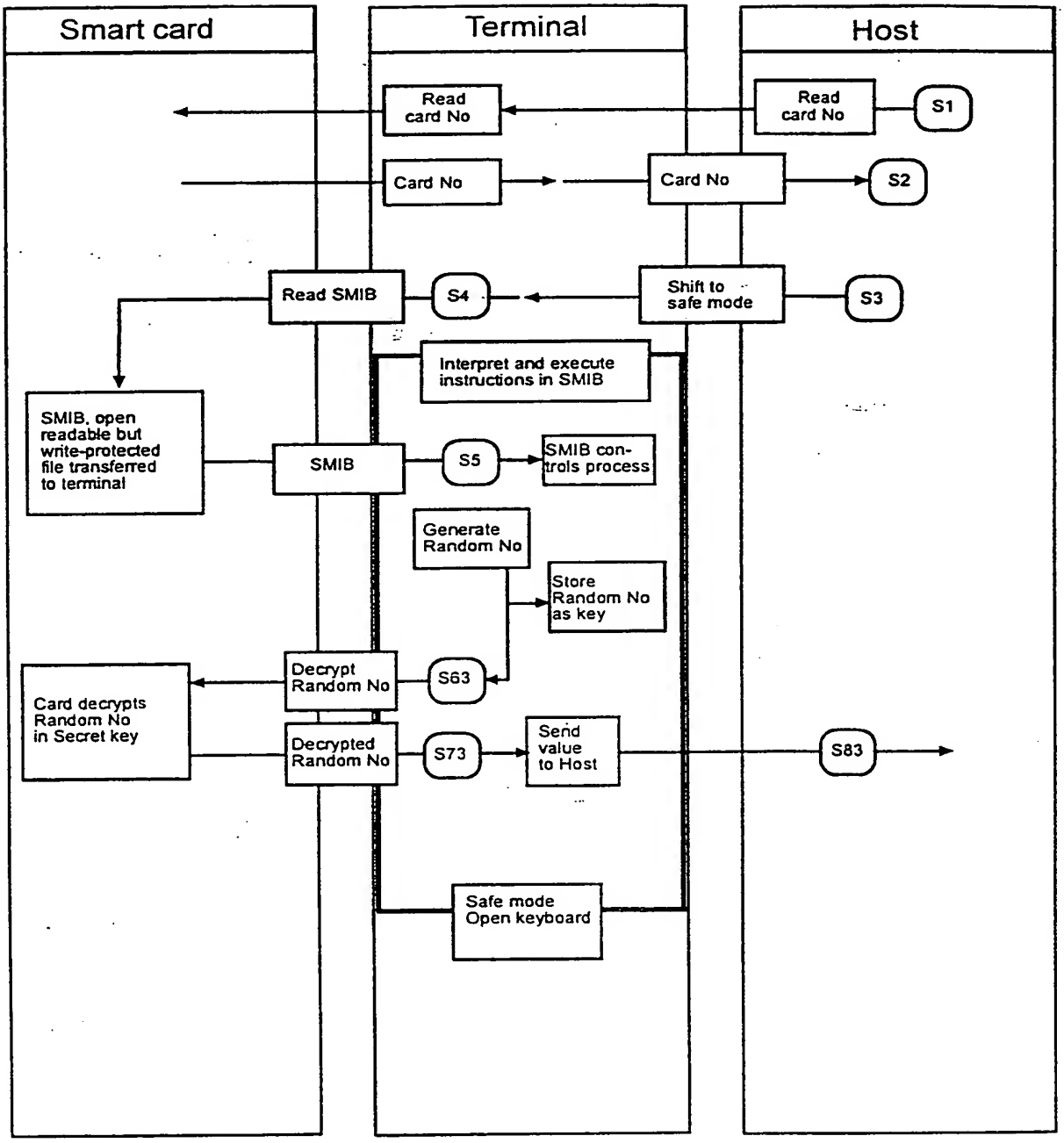

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB controls process
Generate Random No
Store Random No as key
Decrypt Random No
S63
Card decrypts Random No in Secret key
Decrypted Random No
S73
Send value to Host
S83
Safe mode Open keyboard

Fig. 6c

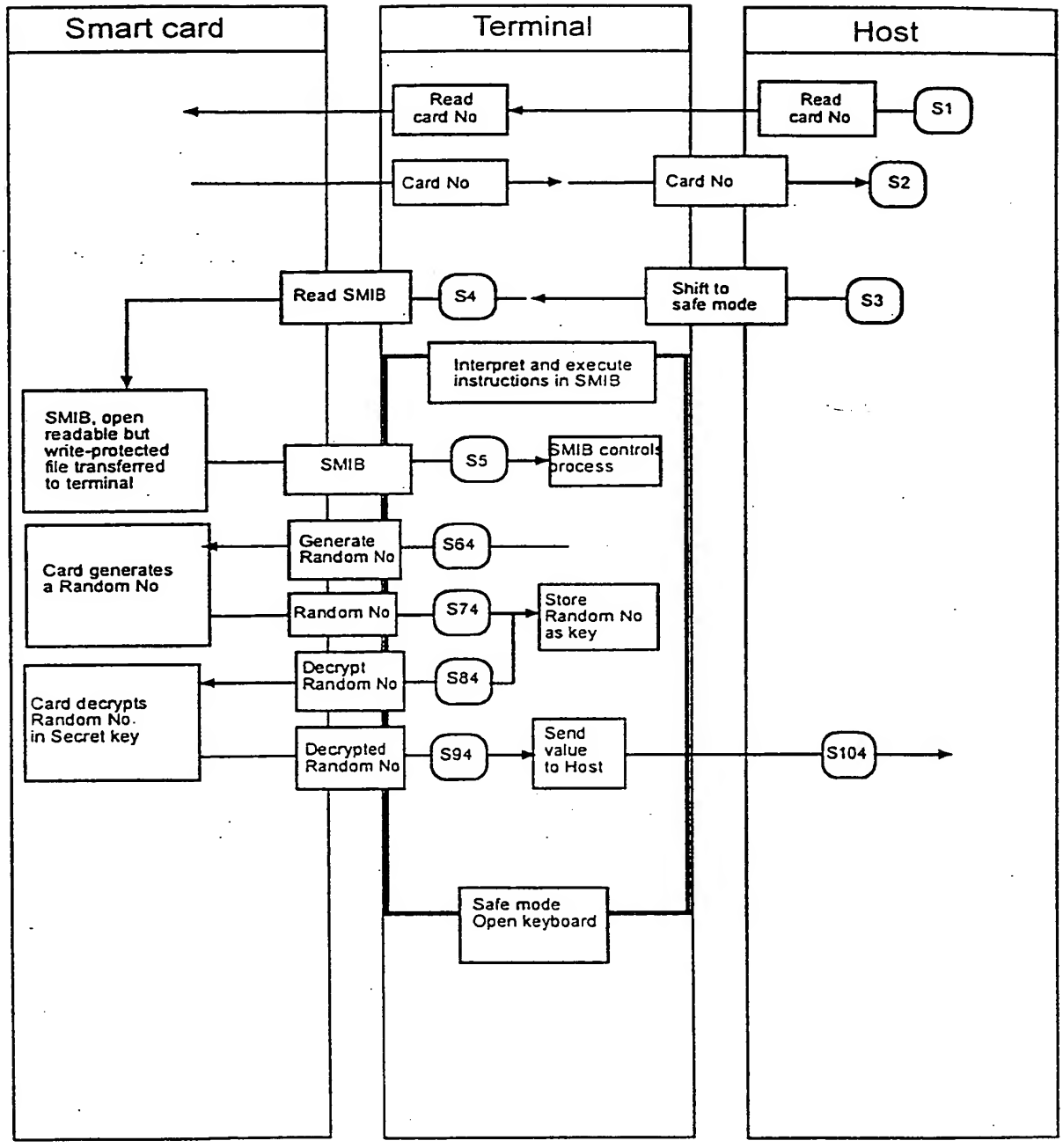

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB controls process
Card generates a Random No
Generate Random No
S64
Random No
S74
Store Random No as key
Card decrypts Random No. in Secret key
Decrypt Random No
S84
Decrypted Random No
S94
Send value to Host
S104
Safe mode Open keyboard

Fig. 6d

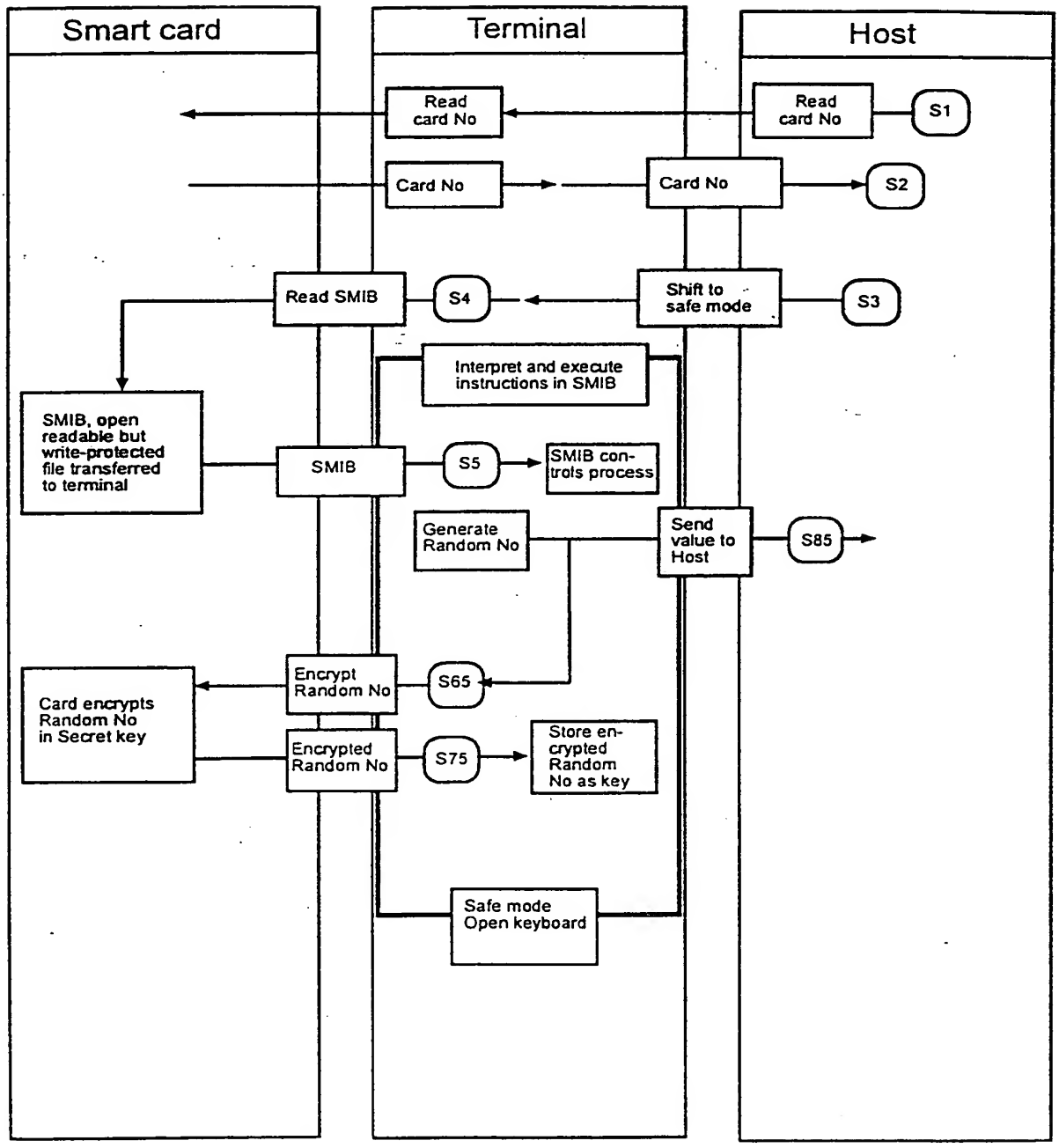

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB controls process
Generate Random No
Send value to Host
S85
Encrypt Random No
S65
Card encrypts Random No in Secret key
Encrypted Random No
S75
Store encrypted Random No as key
Safe mode Open keyboard

Fig. 6e

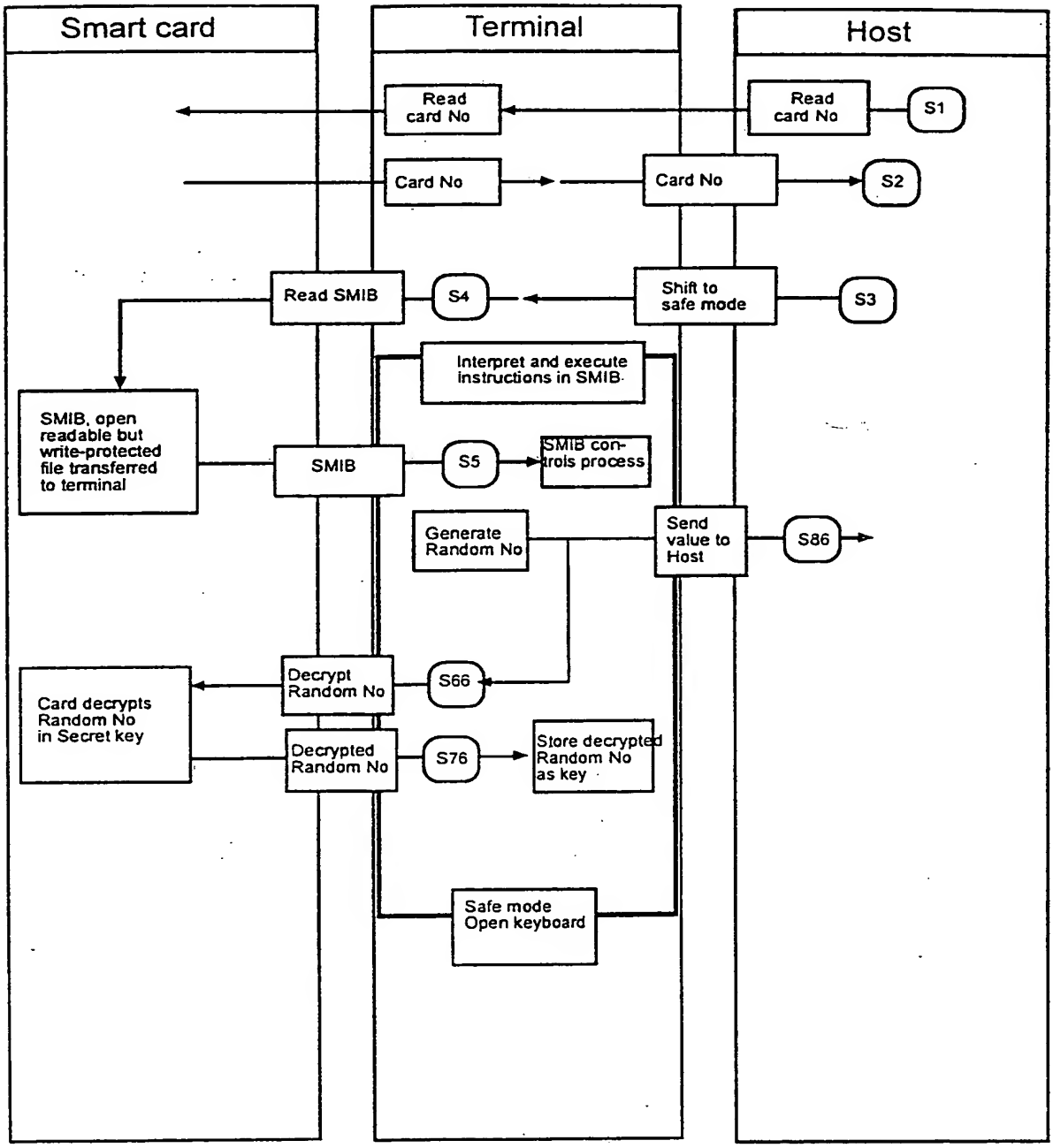

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB controls process
Generate Random No
Send value to Host
S86
Card decrypts Random No in Secret key
Decrypt Random No
S66
Decrypted Random No
S76
Store decrypted Random No as key
Safe mode Open keyboard

Fig. 6f

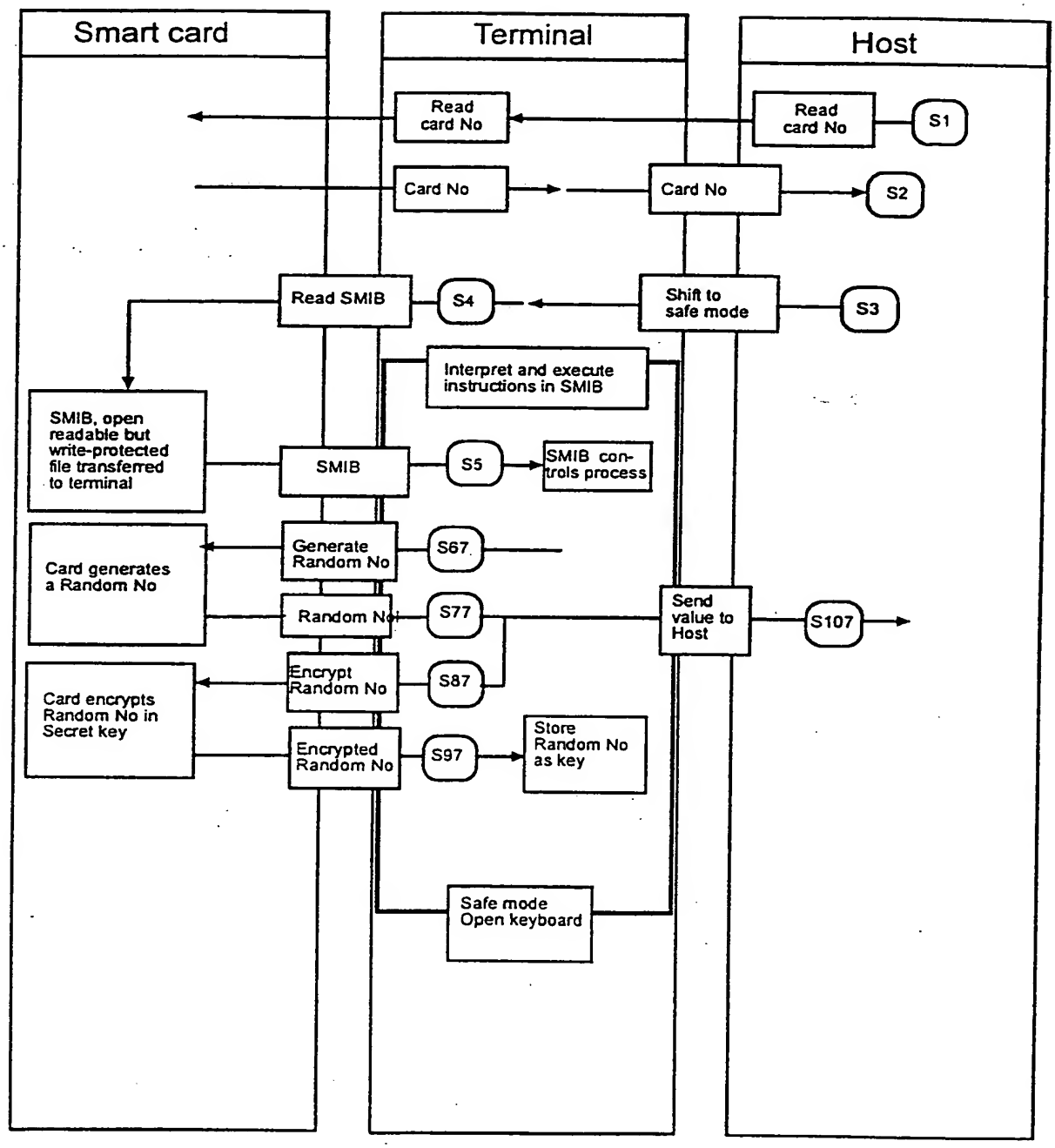

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB controls process
Card generates a Random No
Generate Random No
S67
Random No
S77
Send value to Host
S107
Card encrypts Random No in Secret key
Encrypt Random No
S87
Encrypted Random No
S97
Store Random No as key
Safe mode Open keyboard

Fig. 6g

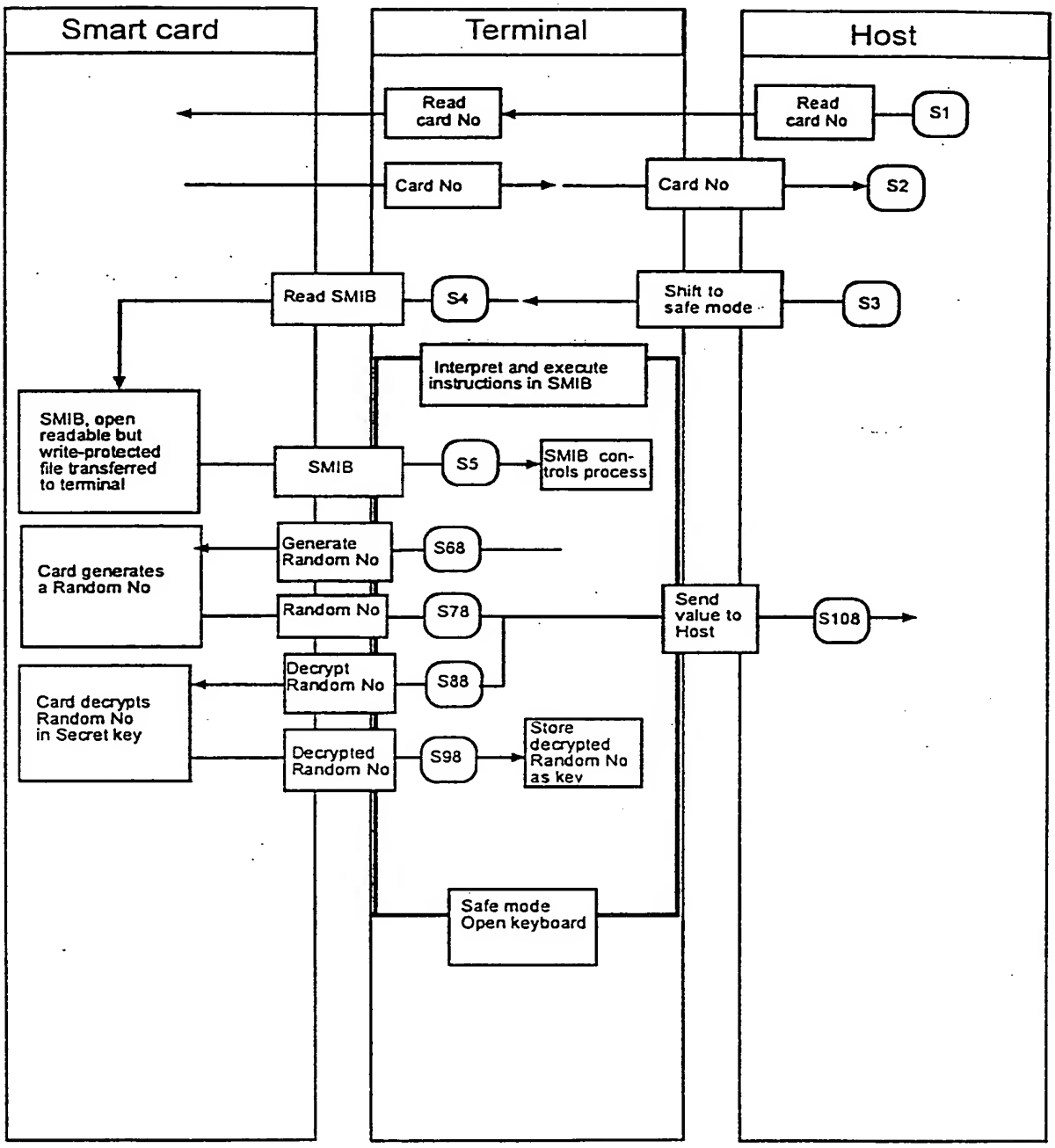

Smart card
Terminal
Host
Read card No
Read card No
S1
Card No
Card No
S2
Read SMIB
S4
Shift to safe mode
S3
Interpret and execute instructions in SMIB
SMIB, open readable but write-protected file transferred to terminal
SMIB
S5
SMIB controls process
Card generates a Random No
Generate Random No
S68
Random No
S78
Send value to Host
S108
Card decrypts Random No in Secret key
Decrypt Random No
S88
Decrypted Random No
S98
Store decrypted Random No as key
Safe mode Open keyboard

Fig. 6h

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 96/01396

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, CLAIMS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5347580 A (REFIK MOLVA ET AL), 13 Sept 1994 (13.09.94), column 1, line 17 - line 24; column 2, line 19 - line 37	1-19
A	GB 2264377 A (ABBUD SALOMON DAHBURA), 25 August 1993 (25.08.93), abstract	1-19
A	US 5109152 A (NOBUYA TAKAGI ET AL), 28 April 1992 (28.04.92), abstract	1-19
A	US 5355413 A (HISASHI OHNO), 11 October 1994 (11.10.94), abstract	1-19

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 February 1997	18 -02- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

03/02/97

International application No.
PCT/SE 96/01396

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 5347580	13/09/94	EP-A- 0566811	27/10/93
GB-A- 2264377	25/08/93	US-A- 5163098	10/11/92
US-A- 5109152	28/04/92	DE-D,T- 68922847	08/02/96
		EP-A,B- 0403656	27/12/90
		JP-A- 2023495	25/01/90
		KR-B- 9400297	14/01/94
		WO-A- 9000781	25/01/90
		JP-A- 2031289	01/02/90
		JP-A- 2031290	01/02/90
		JP-A- 2044389	14/02/90
		JP-A- 2044390	14/02/90
		JP-A- 2044391	14/02/90
US-A- 5355413	11/10/94	DE-A,C- 4306819	09/09/93
		FR-A,B- 2689264	01/10/93
		JP-A- 5250326	28/09/93

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/16 | A3

(11) International Publication Number: WO 99/14888

(43) International Publication Date: 25 March 1999 (25.03.99)

(21) International Application Number: PCT/FI98/00721

(22) International Filing Date: 15 September 1998 (15.09.98)

(30) Priority Data:
973694 15 September 1997 (15.09.97) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: RAIVISTO, Tommi [FI/FI]; Liusketie 16 I 54, FIN–00710 Helsinki (FI).

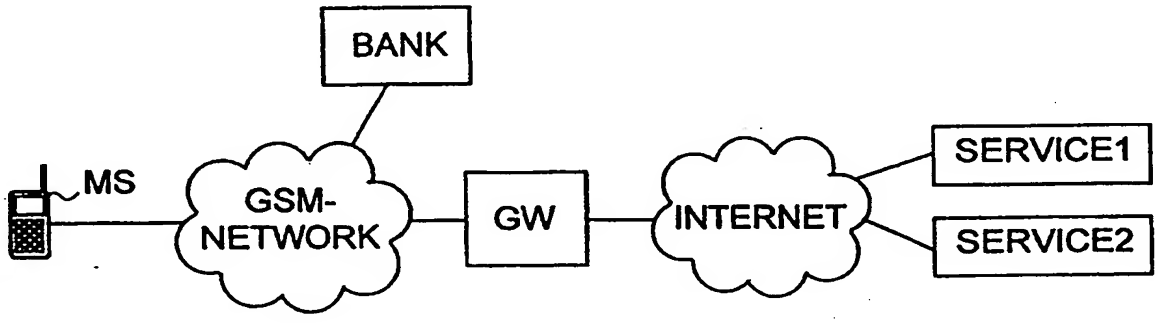
(74) Agent: PATENT AGENCY COMPATENT LTD.; P.O. Box 156, FIN–00511 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(88) Date of publication of the international search report:
3 June 1999 (03.06.99)

(54) Title: SECURITY METHOD FOR TRANSMISSIONS IN TELECOMMUNICATION NETWORKS



(57) Abstract

The invention related to method for providing connection security for the transmission between communicating parties in a telecommunication network, the method comprising the steps of: exchanging security parameters between communicating parties, providing connection security for messages based on these security parameters, and transmitting said messages between communicating parties. It is characteristic for the method according to the invention that it further comprises the steps of: reaching agreement between communicating parties on an interval for recalculation of the security parameters, monitoring of the interval for recalculation by the communicating parties, recalculating the security parameters at the agreed interval, and providing connection security for messages based on the latest recalculated security parameters.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00721

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 9/16
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0189823 A2 (ROHDE & SCHWARZ GMBH & CO. KG), 6 August 1986 (06.08.86), page 3, line 29 - page 5, line 10	1,2,8
A		3-7
	--	
A	WO 9508232 A1 (CHANTILLEY CORPORATION LIMITED), 23 March 1995 (23.03.95), page 8, line 9 - page 9, line 7	1-8
	--	
A	WO 9526087 A1 (CHANTILLEY CORPORATION LIMITED), 28 Sept 1995 (28.09.95), page 2, line 39 - page 3, line 14	1-8
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 March 1999	25 -03- 1999
Name and mailing address of the ISA/ Swedish Patent Office, Box 5055, S-102 42 STOCKHOLM, Facsimile No. + 46 8 666 02 86	Authorized officer: Rune Bengtsson, Telephone No. + 46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 98/00721

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4607137 A (CORNELIS J.A. JANSEN ET AL), 19 August 1986 (19.08.86), see whole document -- --------	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/FI 98/00721

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0189823 A2	06/08/86	DE 3502676 A,C	31/07/86
WO 9508232 A1	23/03/95	AU 7620394 A	03/04/95
		DE 4496863 T	05/12/96
		GB 2296639 A,B	03/07/96
		GB 9405766 D	00/00/00
		GB 9605351 D	00/00/00
		JP 9502845 T	18/03/97
		US 5768381 A	16/06/98
		AU 2076695 A	09/10/95
		DE 19581586 T	28/05/97
		GB 2302246 A,B	08/01/97
		GB 9618811 D	00/00/00
		JP 9510591 T	21/10/97
		US 5832087 A	03/11/98
		WO 9526087 A	28/09/95
WO 9526087 A1	28/09/95	AU 2076695 A	09/10/95
		AU 7620394 A	03/04/95
		DE 4496863 T	05/12/96
		DE 19581586 T	28/05/97
		GB 2296639 A,B	03/07/96
		GB 2302246 A,B	08/01/97
		GB 9605351 D	00/00/00
		GB 9618811 D	00/00/00
		JP 9502845 T	18/03/97
		JP 9510591 T	21/10/97
		US 5768381 A	16/06/98
		US 5832087 A	03/11/98
		WO 9508232 A	23/03/95
US 4607137 A	19/08/86	CA 1220536 A	14/04/87
		EP 0123360 A,B	31/10/84
		SE 0123360 T3	
		JP 1962800 C	25/08/95
		JP 4051105 B	18/08/92
		JP 59207759 A	24/11/84
		NL 8301458 A	16/11/84